REMARKS

Claims 1, 3, 5-8, and 11-29 are all the claims presently pending in the application.

While Applicant believes that all of the claims are patentable over the prior art of record, to expedite prosecution, claims 24, 26, and 27 have been amended to define more clearly the features of the present invention.

Claims 5-8, 11, and 12 have been amended to obviate the Examiner's objection. New claim 29 is added to define more clearly the features of the present invention. No new matter is added.

It is noted that the claim amendments are made only for more particularly pointing out the invention, and not for distinguishing the invention over the prior art, narrowing the claims or for any statutory requirements of patentability. Further, Applicant specifically states that no amendment to any claim herein should be construed as a disclaimer of any interest in or right to an equivalent of any element or feature of the amended claim.

Claims 1, 3, 5-8, and 11-28 stand rejected on prior art grounds.

Claims 1, 3, 5-8, and 11-28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ishiguro (U.S. Patent No. 5,396,558) in view of Urata (U.S. Patent No. 6,799,272) in view of Schneier, "Applied Cryptography: Protocols, Algorithms, and Source Code in C," Second Edition, pps. 466-474 (hereinafter Schneier).

This rejection is respectfully traversed in the following discussion.

I. THE CLAIMED INVENTION

The claimed invention relates to a method and system for producing wise cards.

In an illustrative, non-limiting embodiment of the invention, as defined by independent claim 1, a method of preventing counterfeiting of a smart card includes providing a smart card with a cryptographic structure for authorizing the smart card which cannot be accessed completely by a predetermined small number of readings, wherein said cryptographic structure can be built only by whoever emits the card or an agent thereof.

In conventional methods and systems, counterfeiting/duplication is not rendered difficult since confidential information is carried on the card and an unscrupulous person may find the information simply by looking at or reading the energy construction inside of the card: That is, with a plurality of readings of the card, the information held within the card can be easily detected (e.g., see specification at page 3, line 19, to page 4, line 2).

The claimed invention, on the other hand, complements the conventional smart-card-type of security, which is often all carried on the card itself, by providing extra protection depending on cryptography, with the cryptographic structure (e.g., a key) not being carried by the card and which cannot be accessed completely by a predetermined small number of readings. Moreover, the cryptographic structure can only be built by whoever emits the card or the agent thereof (e.g., see specification at page 4, lines 9-13).

The claimed invention, in addition to preventing the creation of false cards different from the legitimate ones, also prevents the fabrication of clones of a given legitimate smart card. That is, the present invention also provides a mechanism of protection designed to

prevent and/or discourage both copying and creation of new cards (e.g., see specification at page 4, lines 14-17).

II. THE PRIOR ART REJECTION

Claims 1, 3, 5-8, and 11-28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ishiguro in view of Urata in view of Schneier.

Applicants respectfully submit, however, that it would not have been obvious to combine the cited references in the manner alleged in order to arrive at the claimed invention. Moreover, Applicants submit that there are elements of the claimed invention which are not disclosed or suggested by prior art of record, either individually or in combination. Therefore, Applicants respectfully traverse this rejection.

To summarize, the claimed invention has recognized that the unique combination of the features of the claimed invention provides important advantages over the prior art of record, including such teachings as disclosed by each of the individually cited references, Ishiguro, Urata, and Schneier.

In stark contrast to each of the cited prior art of record, the present invention provides a novel and unobvious method of preventing counterfeiting (i.e., false smart cards or illegitimate cards) and/or preventing cloning (i.e., copies of legitimate smart cards or counterfeit smart cards) of a smart card by authorizing (e.g., verifying the legitimacy of) the smart card. That is, the claimed invention provides a simple and effective solution to problems with conventional smart cards.

The claimed invention complements the conventional smart-card-type of security, which is often all carried on the card itself, by providing extra protection depending on cryptography, with the cryptographic structure (e.g., a key) not being carried by the card and which cannot be accessed completely by a predetermined small number of readings. Moreover, the cryptographic structure can only be built by whoever emits the card or the agent thereof (e.g., see specification at page 4, lines 9-13).

In this way, the claimed invention, in addition to preventing the creation of false cards different from the legitimate cards (i.e., illegitimate cards), also prevents the fabrication of clones of a given legitimate smart card. That is, the present invention also provides a mechanism of protection designed to prevent and/or discourage both copying and creation of new cards (e.g., see specification at page 4, lines 14-17).

Accordingly, Applicants respectfully submit that it would not have been obvious to combine the cited references in the manner alleged in order to arrive at the claimed invention.

Indeed, the claimed invention has recognized that the unique combination of the features of the claimed invention provides important advantages over the prior art of record, including such teachings as disclosed by each of the individually cited references, Ishiguro, Urata, and Schneier.

For example, the claimed invention, as exemplarily defined by independent claim 1, provides a method of preventing counterfeiting of a smart card, including:

> *providing a smart card with a cryptographic structure for authorizing the smart card which cannot be accessed completely by a predetermined small number of readings,*

wherein said cryptographic structure can be built only by whoever emits the card or an agent thereof;

providing a reader for reading said smart card and including a database holding information related to unauthorized smart cards, said reader being on-line, such that said reader is operatively connected to a network, only when said database of said reader is being updated by said network,

wherein said reader includes a random number generator, which, when a card is read, chooses a pair (a, b) of distinct numbers with a < b between 1 and N,

wherein said smart card carries thereon predetermined N channels as C1, C2,..., CN, where N is an integer,

wherein each channel Ci, with i equal to 1, 2, ..., N, carries a pair of numbers (hi, li), and

wherein hi is the i^{th} high number and li is the i^{th} low number,

wherein said reader obtains a content of only two of said channels, and

periodically communicating, by said reader of said smart card, with a database where a predetermined characteristic of the card is checked (emphasis added).

The Ishiguro Reference

In comparison, Ishiguro discloses a method and apparatus for the payment of charges by IC cards which eliminate the need for communication between the management center and the IC card terminal each time the card user inserts his IC card into the latter to get his desired service and which permit detection of abuse of a forged IC card or intentionally altered IC card terminal.

In Ishiguro, the IC card has prestored in its memory means a master public key nA for verifying a master digital signature SA, a card identification number IDU for specifying the IC card and a first master digital signature SA1 for information containing at least the card identification number IDU. On the other hand, in Ishiguro, the IC card terminal has prestored in its terminal memory the above-mentioned master public key nA, a terminal identification number IDT for specifying the IC card terminal and a second master digital

signature SA2 for information including at least the above-mentioned terminal identification number IDT (see Ishiguro at column 2, lines 17-61).

In Ishiguro, the method includes:

1) a step wherein the IC card transmits at least the card identification number IDU and the first master digital signature SA1 to the IC card terminal;

2) a step wherein the IC card terminal verifies the validity of the first master digital signature SA1 through use of the master public key nA and the card identification number IDU received from the IC card;

3) a step wherein when the first master digital signature SA1 is valid, the IC card terminal transmits at least the terminal identification number IDT and the second master digital signature SA2 to the IC card;

4) a step wherein the IC card verifies the validity of the second master digital signature SA2 through use of the master public key nA and the terminal identification number IDT received from the IC card terminal; and

5) a step wherein when the second master digital signature SA2 is valid, the IC card terminal generates a value V corresponding to the charge for a service specified by the IC card after the service is provided.

Thus, Ishiguro clearly does not disclose or suggest a method "*wherein said smart card carries thereon predetermined N channels as C1, C2,..., CN, where N is an integer, wherein each channel Ci, with i equal to 1, 2, ..., N, carries a pair of numbers (hi, li), and*

wherein hi is the ith high number and li is the ith low number, wherein said reader obtains a content of only two of said channels", as recited, for example, in independent claim 1.

The Urata Reference

However, the Examiner turns to Urata to make up for the deficiencies of Ishiguro.

The Examiner alleges that Urata discloses wherein the smart card carries thereon predetermined N channels as C1, C2,..., CN, where N is an integer, wherein each channel Ci, with i equal to 1, 2, ..., N, carries a pair of numbers (hi, li), and wherein hi is the ith high number and li is the ith low number (citing Urata at column 2, lines 32-52 and Figure 1, 106, 128, and 142). The Examiner also alleges that the Urata discloses that the reader obtains a content of only two of the channels (citing Urata at column 2, lines 37-47).

However, Applicant respectfully disagrees with the Examiner's position.

Contrary to the Examiner's position, Applicants submit that Urata does not disclose or suggest at least that channel Ci carries a pair of numbers (hi, li), "*wherein hi is the ith high number and li is the ith low number*", as recited in claim 1.

Instead, column 2, lines 32-52 and Figure 1 of Urata merely discloses that:

> The problems associated with remote device authentication are reduced or overcome by an arrangement in accordance with the principles of the invention in which a remote device and an authentication center each store an identical key code index which includes a plurality of key code numbers. The remote device and authentication center communicate with each other through first and second keys, that each specify a particular key code number from the key code index. Specifically, the remote device translates the first key received from the authentication center to determine the particular key code number and then generates a second key also specifying the particular key code number. Thereafter, the authentication center translates the second key to determine a second key code and compares the first and second key code numbers. If the two key code numbers match, the remote device is authenticated.

> The remote device may be, for example, (1) a wireless telephone, (2) a smartcard or (3) a credit card used in conjunction with an Internet access device such as a personal computer (PC) and the authentication center may be, for example, a wireless base station or a credit/smartcard authentication center.

Thus, Applicants respectfully submit that Urata does not make up for the deficiencies of Ishiguro.

Moreover, Applicants respectfully submit that it would not have been obvious to combine the cited references in the manner alleged in order to arrive at the claimed invention, since such a combination would require a substantial reconstruction of the Ishiguro reference.

It is noted that, if the proposed modification or combination of the prior art would change the principle of operation of the prior art invention being modified, then the teachings of the reference are not sufficient to render the claims *prima facie* obvious (see In re Ratti, 270 F.2d 810, 123 USPQ 349 (CCPA 1959).

As mentioned above, Ishiguro discloses **1)** a step wherein the IC card transmits at least the card identification number IDU and the first master digital signature SA1 to the IC card terminal; **2)** a step wherein the IC card terminal verifies the validity of the first master digital signature SA1 through use of the master public key nA and the card identification number IDU received from the IC card; **3)** a step wherein when the first master digital signature SA1 is valid, the IC card terminal transmits at least the terminal identification number IDT and the second master digital signature SA2 to the IC card; **4)** a step wherein the IC card verifies the validity of the second master digital signature SA2 through use of the master public key nA and the terminal identification number IDT received from the IC card

terminal; and **5)** a step wherein when the second master digital signature SA2 is valid, the IC card terminal generates a value V corresponding to the charge for a service specified by the IC card after the service is provided.

In contrast, Urata discloses a remote device and an authentication center each store an identical key code index which includes a plurality of key code numbers. The remote device and authentication center communicate with each other through first and second keys, that each specify a particular key code number from the key code index. The remote device translates the first key received from the authentication center to determine the particular key code number and then generates a second key also specifying the particular key code number. Thereafter, the authentication center translates the second key to determine a second key code and compares the first and second key code numbers. If the two key code numbers match, the remote device is authenticated.

Applicants submit that modifying Ishiguro to include the features of Urata would obviate the method steps of the Ishiguro invention. That is, should the method of Urata be used to replace the method of Ishiguro, then Ishiguro would be completely different from its disclosed form. Indeed, such would change the principle of operation of the method of Ishiguro, and thus, would not be sufficient to render the claims *prima facie* obvious.

Thus, for at least the foregoing reasons, Applicants respectfully submit that it would not have been obvious to combine prior art of record to arrive at the claimed invention, since such would require changing the principle of operation of the primary reference, Ishiguro.

Moreover, for the reasons set forth above, Applicants also submit that there are elements of the claimed invention which are not disclosed or suggested by the prior art of record, alone or in combination.

Therefore, Applicants respectfully request that the Examiner reconsider and withdraw this rejection.

III. FORMAL MATTERS

Claims 5-8, 11, and 12 have been objected to by the Examiner. These claims have been amended to obviate this objection.

Therefore, the Examiner is requested to reconsider and withdraw this objection.

IV. CONCLUSION

In view of the foregoing, Applicants submit that claims 1, 3, 5-8, and 11-29, all the claims presently pending in the application, are patentably distinct over the prior art of record and are in condition for allowance. The Examiner is respectfully requested to pass the above application to issue at the earliest possible time.

Should the Examiner find the application to be other than in condition for allowance, the Examiner is requested to contact the undersigned at the local telephone number listed below to discuss any other changes deemed necessary in a telephonic or personal interview.

RECEIVED
CENTRAL FAX CENTER
SEP 0 7 2006

The Commissioner is hereby authorized to charge any deficiency in fees or to credit any overpayment in fees to Assignee's Deposit Account No. 50-0510.

Respectfully Submitted,

Date: September 7, 2006

John J. Dresch, Esq.
Registration No. 46,672

Sean M. McGinn, Esq.
Registration No. 34,386

MCGINN INTELLECTUAL PROPERTY LAW GROUP, PLLC
8321 Old Courthouse Road, Suite 200
Vienna, Virginia 22182-3817
(703) 761-4100
Customer No. 48150

CERTIFICATE OF TRANSMISSION

I certify that I transmitted via facsimile to (571) 273-8300 the enclosed Amendment under 37 C.F.R. § 1.111 to Examiner Brandon S. Hoffman, Art Unit 2136, on September 7, 2006.

John J. Dresch, Esq.
Registration No. 46,672
Sean M. McGinn, Esq.
Registration No. 34,386